What is claimed is:

1. An apparatus for maintaining the privacy of a plaintext message transmitted over a non-secure channel between a transmitting party and a receiving party without cryptographic key exchange between said parties, comprising:

(a) first transformation means for embodying the plaintext message in a non-reversible first output;

(b) second transformation means for generating a second output which is a reversible second transformation of said first output, such that said second output is non-reversible;

(c) first transmitting means for transmitting said second output from the transmitting party to the receiving party;

(d) third transformation means for generating a third output which is a reversible third transformation of said second output, such that said third output is non-reversible;

(e) second transmitting means for transmitting said third output from the receiving party to the transmitting party;

(f) reverse second transformation means for generating a fourth output through reversal of the second transformation applied to said third output, such that said fourth output is non-reversible;

(g) third transmitting means for transmitting said fourth output from the transmitting party to the receiving party;

(h) reverse third transformation means for generating said first output through reversal of the third transformation applied to said fourth output; and

(i) extracting means for extracting the plaintext message from said first output in the possession of the receiving party.

2. An apparatus according to claim 1, wherein said first transmitting means is also said third transmitting means.

3. An apparatus according to claim 1, wherein

(a) said first transformation means comprises a first mathematical function creating an embodiment of the plaintext message in a non-invertible first output;

(b) said second transformation means comprises an invertible second mathematical function;

(c) said third transformation means comprises an invertible third mathematical function;

(d) said reverse second transformation means comprises the inverse of said second mathematical function; and

(e) said reverse third transformation means comprises the inverse of said third mathematical function.

4. A method for securely transmitting a plaintext message from a transmitting party to a receiving party over a non-secure channel, comprising the steps of:

(a) generating a first transformation of the plaintext message such that the plaintext message is embodied in a first output of said first transformation and said first output of said first transformation is non-reversible;

(b) generating a reversible second transformation of said first output of said first transformation such that a second output of said second transformation is non-reversible;

(c) transmitting said second output of said second transformation from the transmitting party to the receiving party;

(d) generating a reversible third transformation of said second output of said second transformation such that a third output of said third transformation is non-reversible;

(e) transmitting said third output of said third transformation from the receiving party to the transmitting party;

(f) reversing said second transformation on said third output of said third transformation such that a fourth output of said reversal of the second transformation is non-reversible;

(g) transmitting said fourth output of said reversal of the second transformation from the transmitting party to the receiving party;

(h) reversing said third transformation on said fourth output to yield said first output of said first transformation; and

(i) extracting the plaintext message from said first output.

5. A method according to claim 4, wherein said first transmitting means is also said third transmitting means.

6. A method according to claim 4, wherein:

(a) said first transformation comprises a first mathematical function creating an embodiment of the plaintext message in a non-invertible first output;

(b) said second transformation comprises an invertible second mathematical function;

(c)said third transformation comprises an invertible third mathematical function;

(d) said reverse second transformation comprises the inverse of said second mathematical function; and

(e) said reverse third transformation comprises the inverse of said third mathematical function .

7. An apparatus for maintaining the privacy of a plaintext message conveyed over a non-secure channel between a transmitting party and a receiving party wherein:

(a) the transmitting party neither possesses nor uses any cryptographic key that was created by the receiving party;

(b) the receiving party neither possesses nor uses any cryptographic key, that was created by the transmitting party;

(c) neither the transmitting party nor the receiving party exchanged a cryptographic key with the other party, and

(d) the plaintext message is transmitted to and understood by the receiving party, but cannot be understood by any third party who was privy to all transmissions between the transmitting party and the receiving party.

8. A method for maintaining the privacy of a plaintext message conveyed over a non-secure channel between a transmitting party and a receiving party wherein:

(a) the transmitting party neither possesses nor uses any cryptographic key, that was created by the receiving party;

(b) the receiving party neither possesses nor uses any cryptographic key, that was created by the transmitting party;

(c) neither the transmitting party nor the receiving party exchanged a cryptographic key, with the other party and

(d) the plaintext message is transmitted to and understood by the receiving party, but cannot be understood by any third party who was privy to all transmissions between the transmitting party and the receiving party.

9. An apparatus according to claim 1, wherein said plaintext message comprises a cryptographic key.

10. A method according to claim 4, wherein said plaintext message comprises a cryptographic key.